FIG. 1

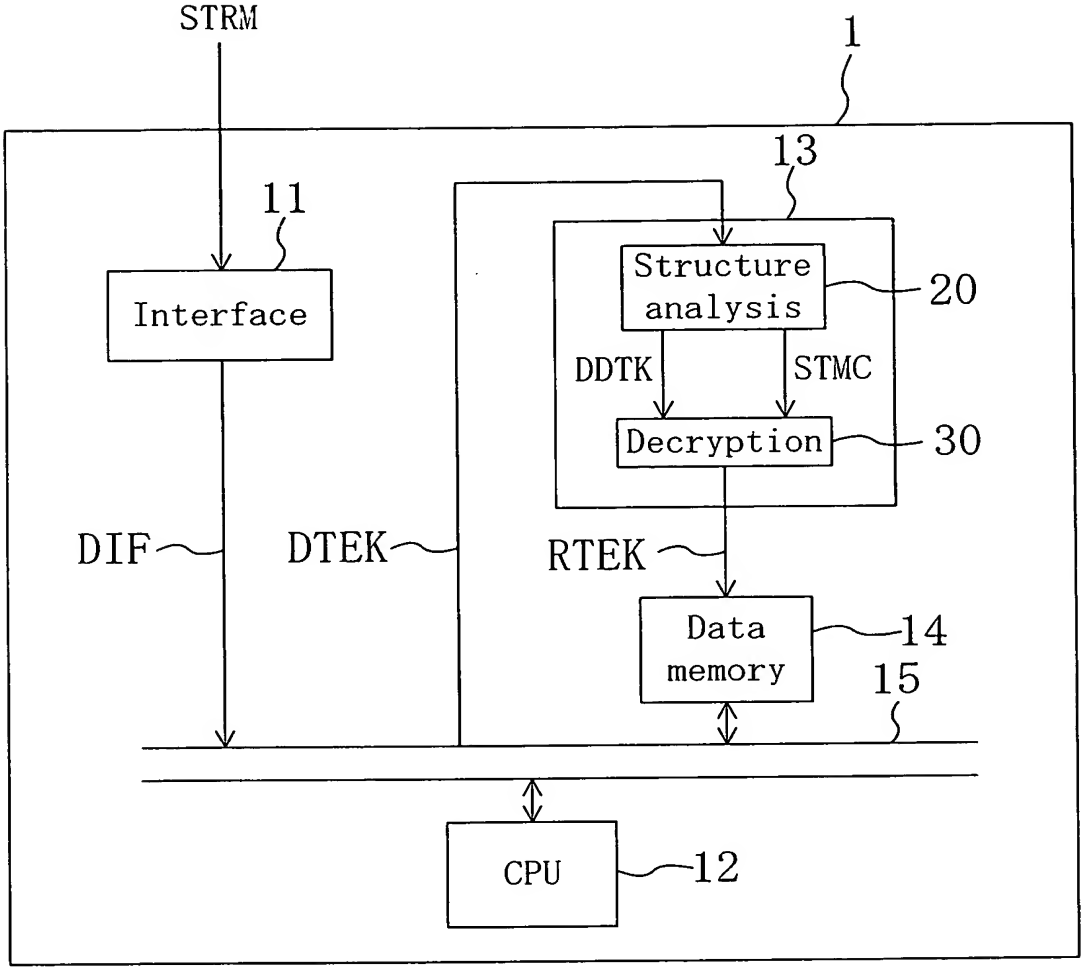

STRM
1
13
11
Interface
Structure analysis
20
DDTK
STMC
Decryption
30
DIF
DTEK
RTEK
Data memory
14
15
CPU
12

FIG. 2

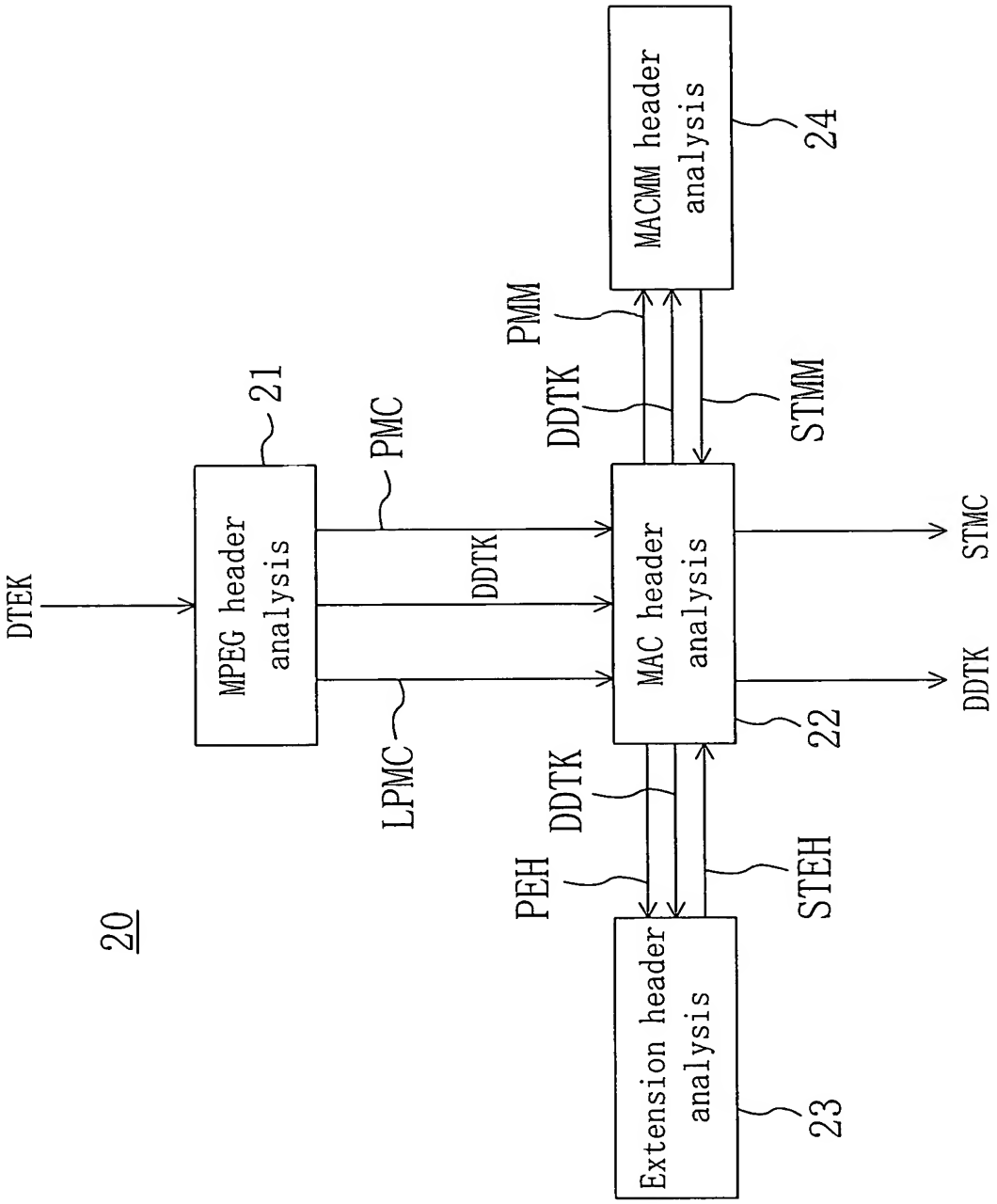

20
DTEK
MPEG header analysis
21
PMC
DDTK
LPMC
MAC header analysis
22
STMC
DDTK
PMM
DDTK
STMM
MACMM header analysis
24
PEH
DDTK
STEH
Extension header analysis
23

FIG. 3

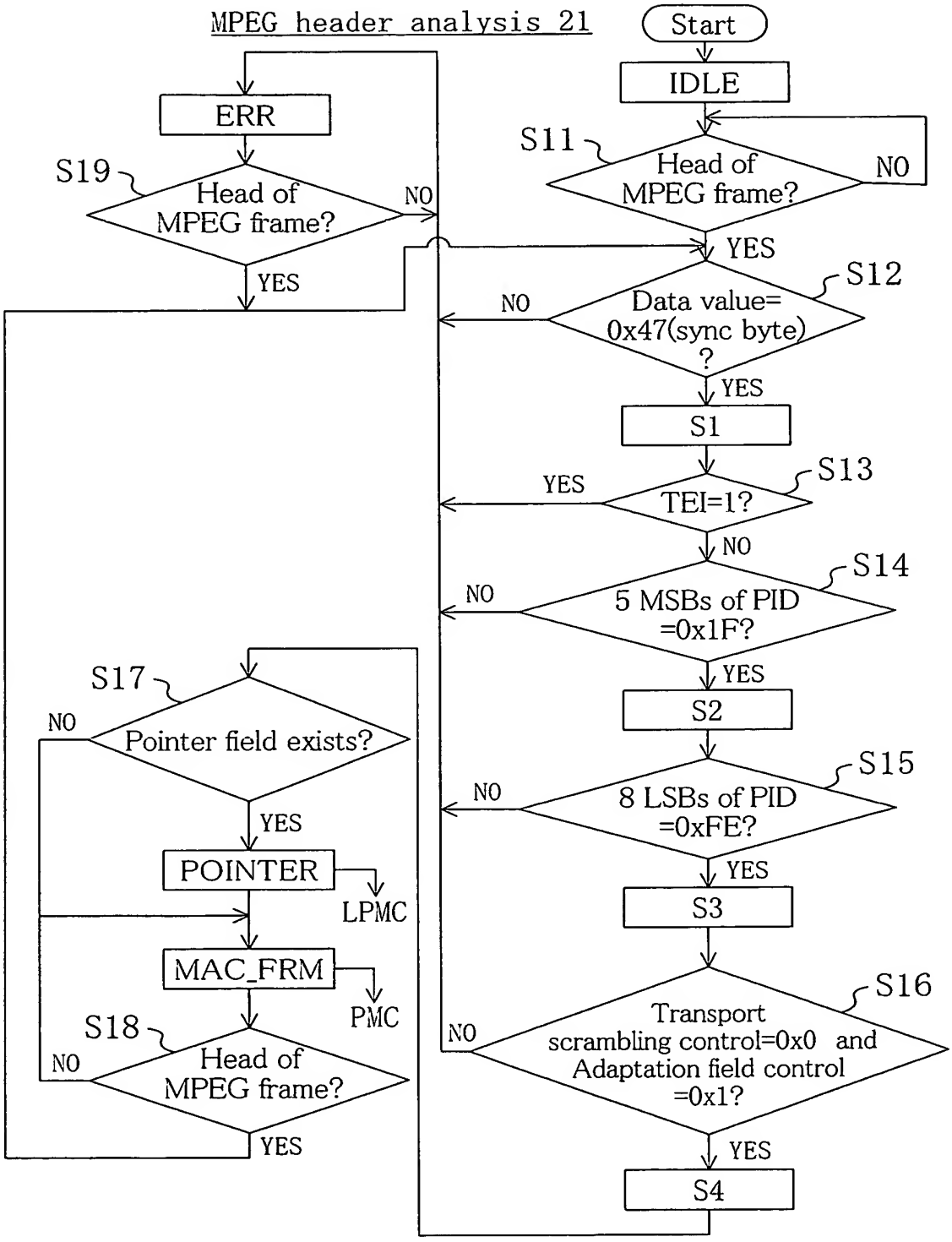

MPEG header analysis 21
Start
IDLE
S11
Head of MPEG frame?
NO
YES
S12
Data value= 0x47(sync byte) ?
NO
YES
S1
S13
TEI=1?
YES
NO
S14
5 MSBs of PID =0x1F?
NO
YES
S2
S15
8 LSBs of PID =0xFE?
NO
YES
S3
S16
Transport scrambling control=0x0 and Adaptation field control =0x1?
NO
YES
S4
ERR
S19
Head of MPEG frame?
NO
YES
S17
Pointer field exists?
NO
YES
POINTER
LPMC
MAC_FRM
PMC
S18
Head of MPEG frame?
NO
YES

FIG. 4

Field	Length (bit)	Description
sync byte	8	0x47:MPEG Packet Sync Byte
transport error indicator (TEI)	1	0…No error in packet 1…Error in packet
payload unit start indicator (PUSI)	1	0…No pointer field exists 1…Pointer field exists *Pointer field is 5th byte of MPEG frame PUSI is set when corresponding packet includes start of payload
transport priority	1	0(Reserved)
PID	13	0x1FFE for DOCSIS Data-Over-Cable
transport scrambling control	2	0(Reserved)
adaptation field control	2	1(This field unavailable for DOCSIS PID)
continuity counter	4	Circular counter of PID

FIG. 5

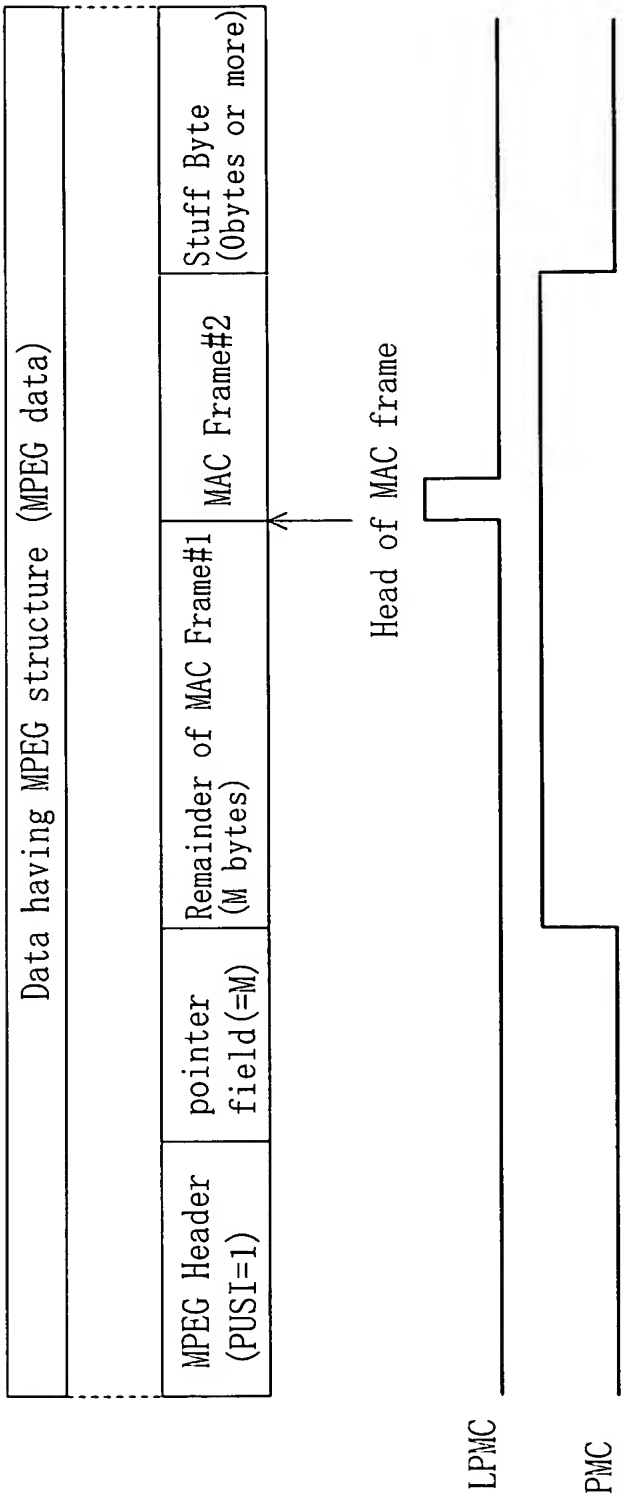

Data having MPEG structure (MPEG data)
MPEG Header (PUSI=1)
pointer field(=M)
Remainder of MAC Frame#1 (M bytes)
MAC Frame#2
Stuff Byte (Obytes or more)
Head of MAC frame
LPMC
PMC

FIG. 6

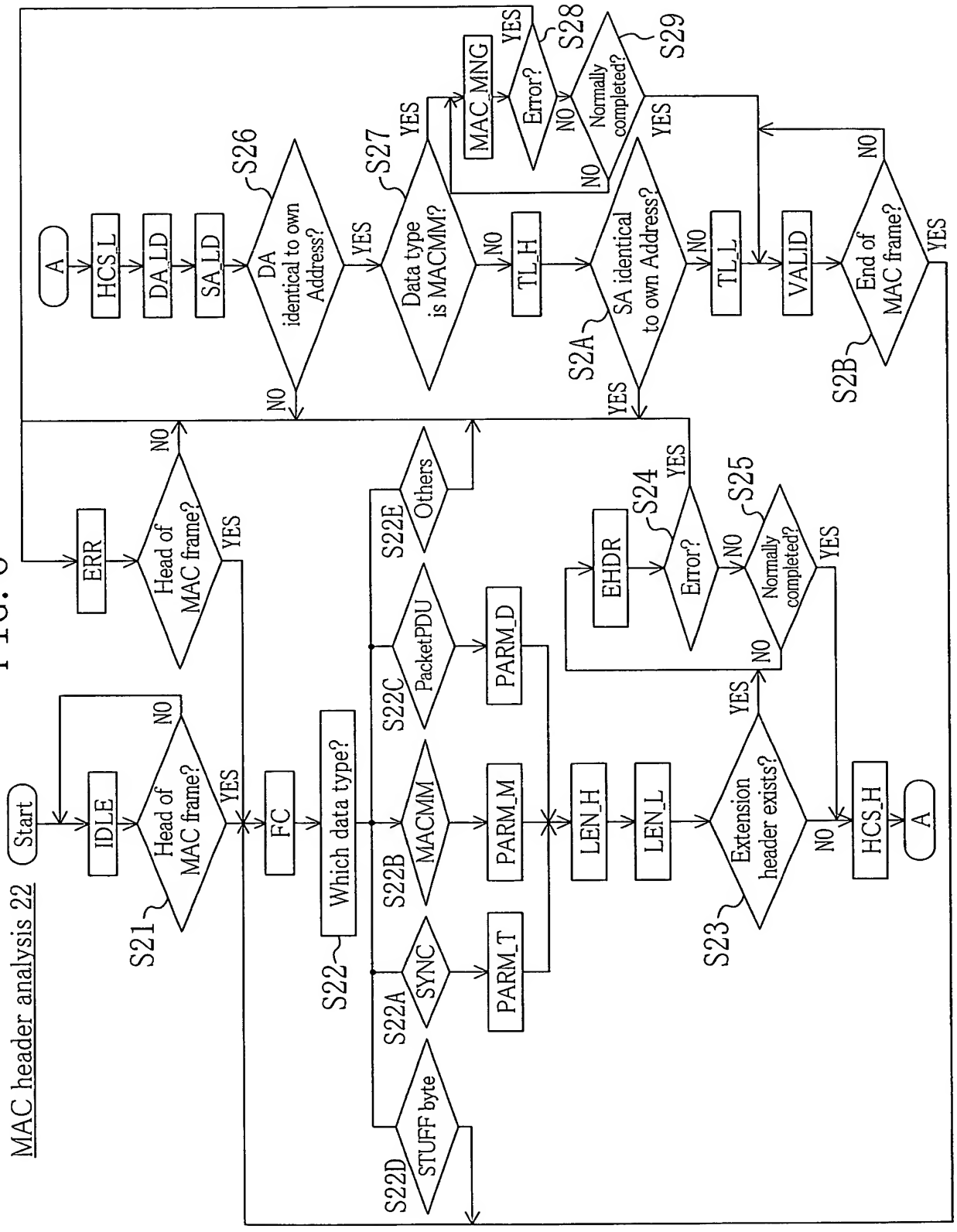

MAC header analysis 22
Start
IDLE
Head of MAC frame?
NO
YES
S21
FC
Which data type?
S22
S22A
SYNC
S22B
MACM
S22C
PacketPDU
S22D
STUFF byte
S22E
Others
PARM_T
PARM_M
PARM_D
LEN_H
LEN_L
Extension header exists?
S23
HCS_H
A
EHDR
Error?
S24
Normally completed?
S25
ERR
Head of MAC frame?
A
HCS_L
DA_LD
SA_LD
DA identical to own Address?
S26
Data type is MACMM?
S27
MAC_MNG
Error?
S28
Normally completed?
S29
TL_H
SA identical to own Address?
S2A
TL_L
VALID
End of MAC frame?
S2B

FIG. 7

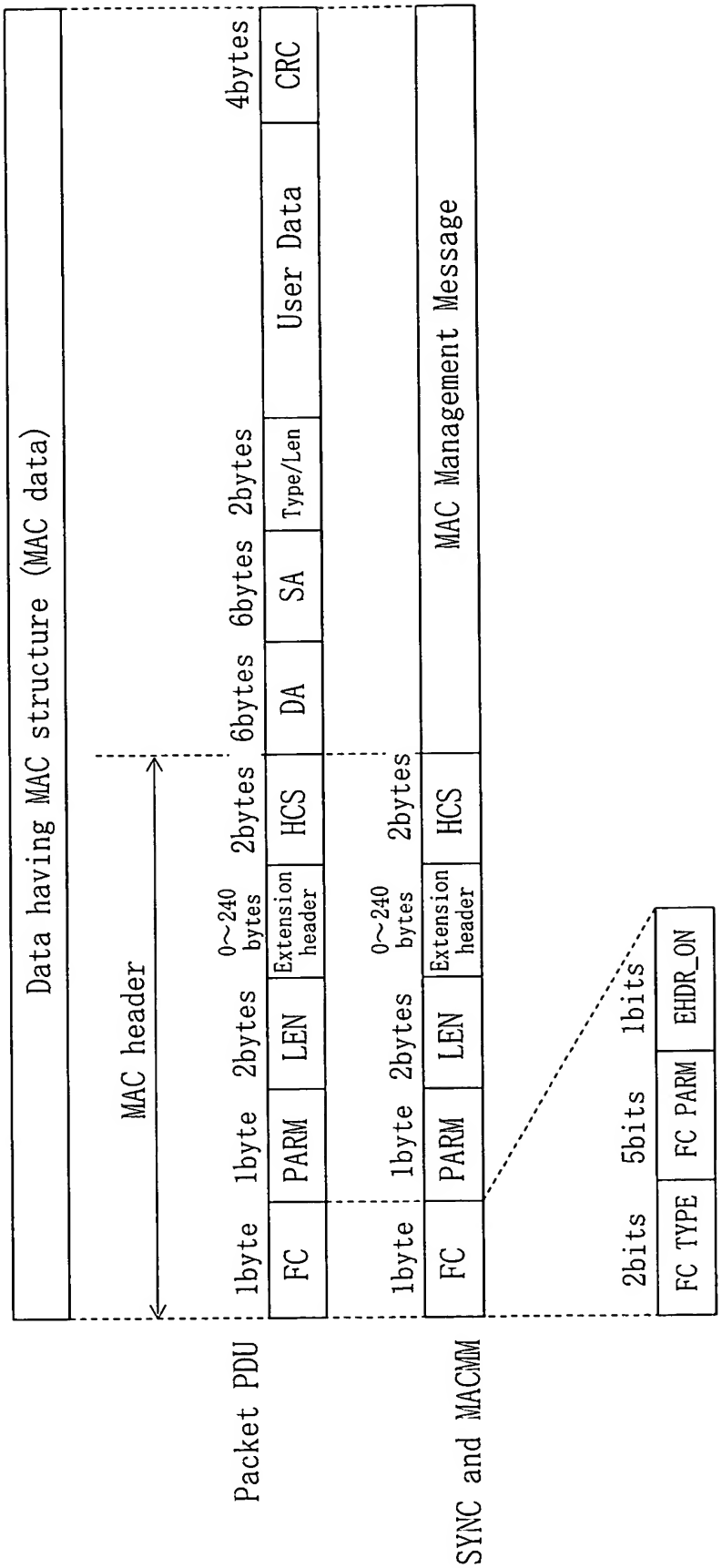

Data having MAC structure (MAC data)
MAC header
Packet PDU
1byte
FC
1byte
PARM
2bytes
LEN
0~240 bytes
Extension header
2bytes
HCS
6bytes
DA
6bytes
SA
2bytes
Type/Len
User Data
4bytes
CRC
SYNC and MACMM
1byte
FC
1byte
PARM
2bytes
LEN
0~240 bytes
Extension header
2bytes
HCS
MAC Management Message
2bits
FC TYPE
5bits
FC PARM
1bits
EHDR_ON

FIG. 8

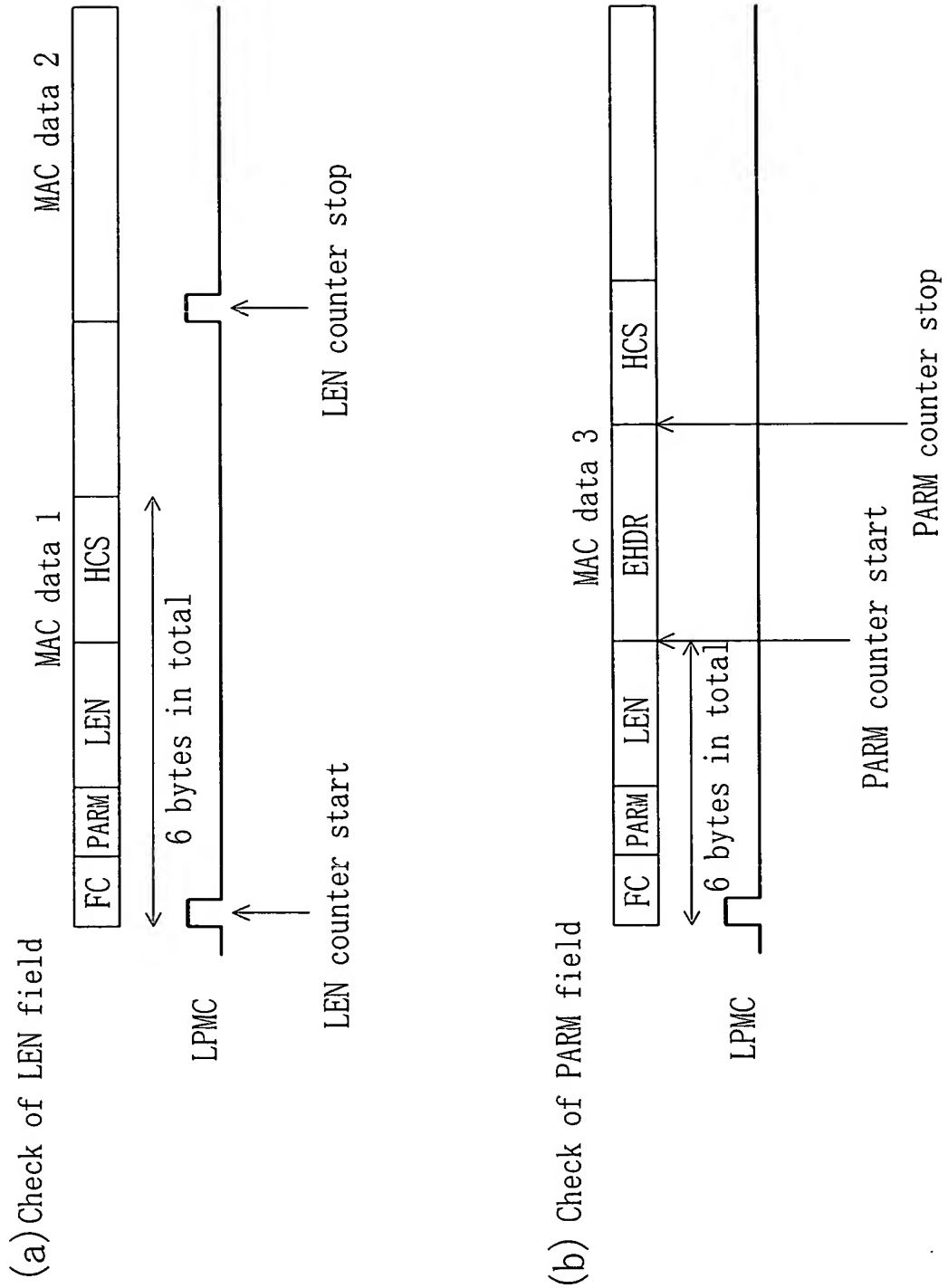

(a) Check of LEN field
MAC data 1
MAC data 2
FC
PARM
LEN
HCS
6 bytes in total
LPMC
LEN counter start
LEN counter stop
(b) Check of PARM field
MAC data 3
FC
PARM
LEN
EHDR
HCS
6 bytes in total
LPMC
PARM counter start
PARM counter stop

FIG. 9

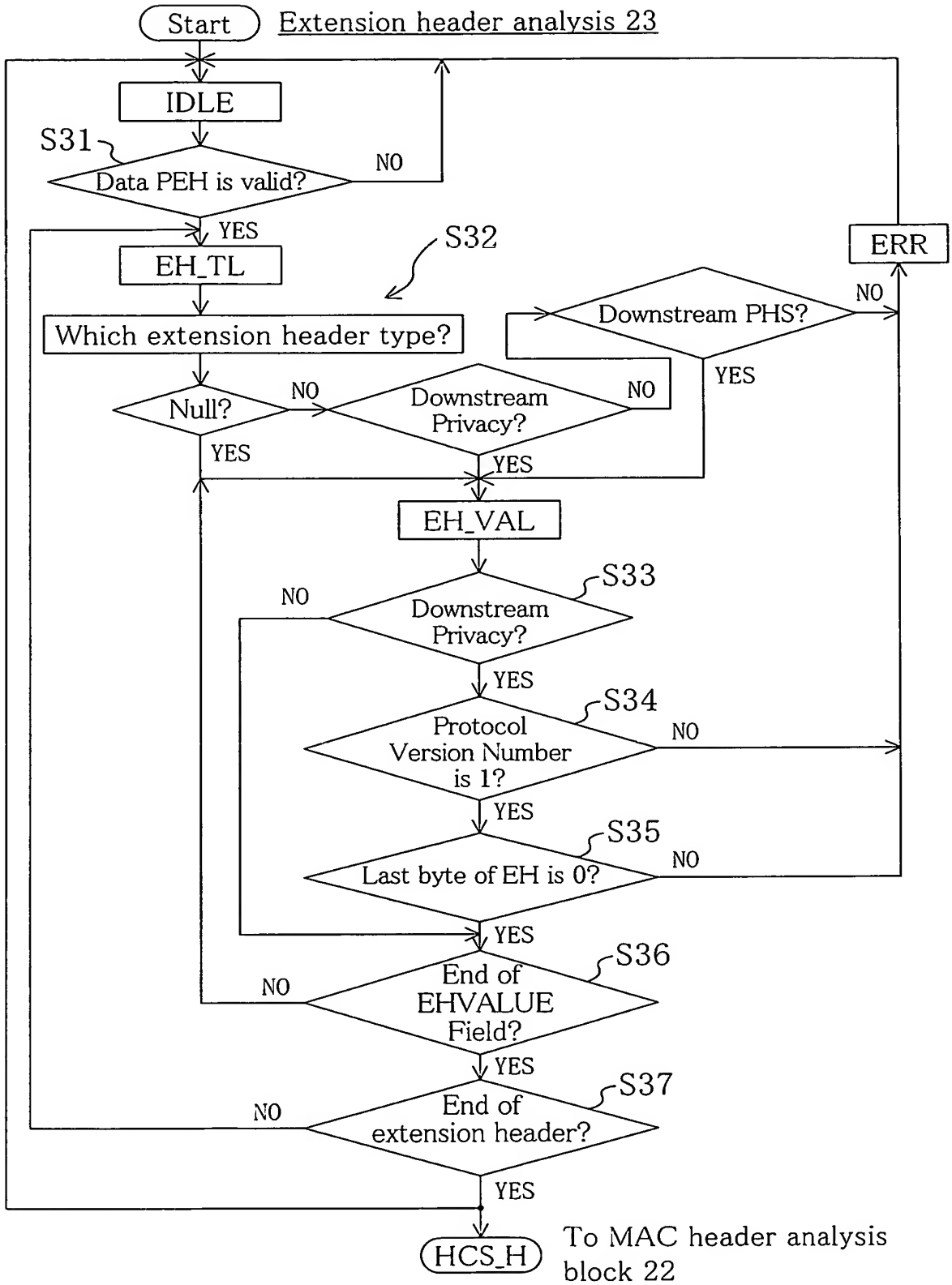

Start
Extension header analysis 23
IDLE
S31
Data PEH is valid?
NO
YES
EH_TL
S32
Which extension header type?
Null?
NO
Downstream Privacy?
NO
YES
YES
ERR
Downstream PHS?
NO
YES
EH_VAL
S33
NO
Downstream Privacy?
YES
S34
Protocol Version Number is 1?
NO
YES
S35
Last byte of EH is 0?
NO
YES
S36
NO
End of EHVALUE Field?
YES
S37
NO
End of extension header?
YES
HCS_H
To MAC header analysis block 22

FIG. 10

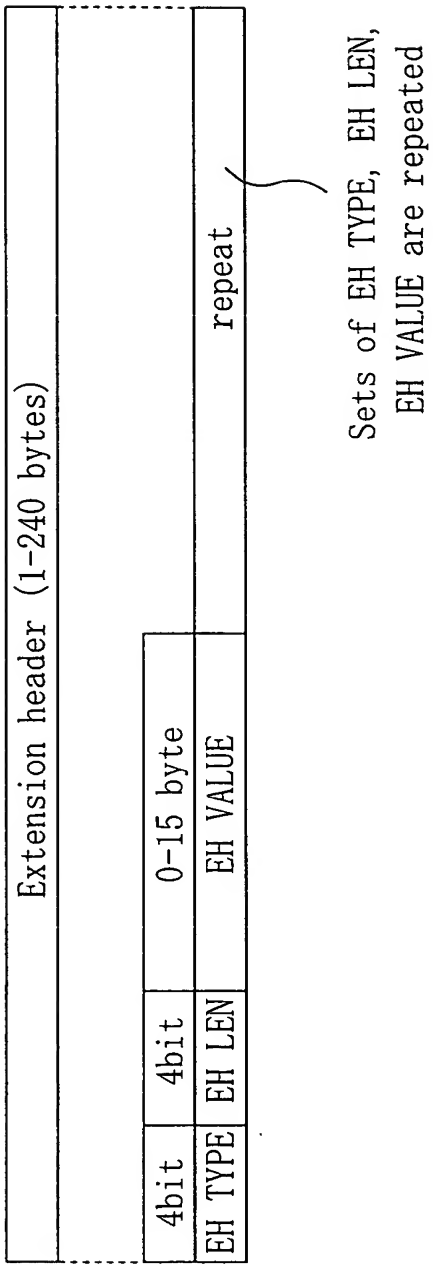

Extension header (1-240 bytes)
4bit
4bit
0-15 byte
EH TYPE
EH LEN
EH VALUE
repeat
Sets of EH TYPE, EH LEN, EH VALUE are repeated

FIG. 11

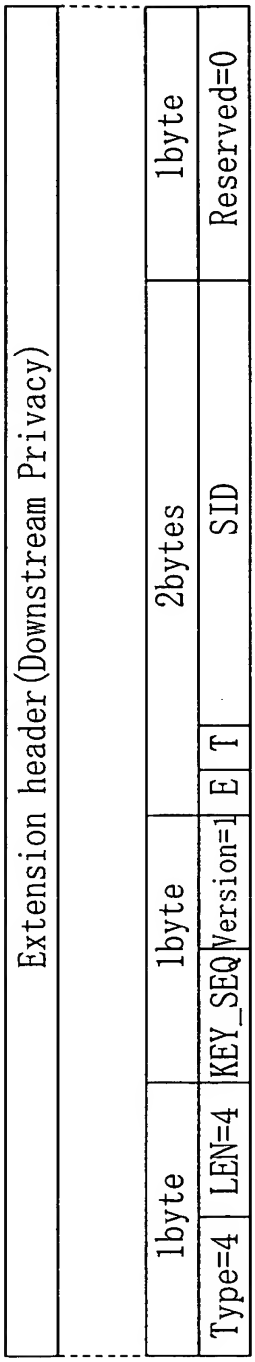

Extension header(Downstream Privacy)
1byte
1byte
2bytes
1byte
Type=4
LEN=4
KEY_SEQ
Version=1
E
T
SID
Reserved=0

FIG. 12

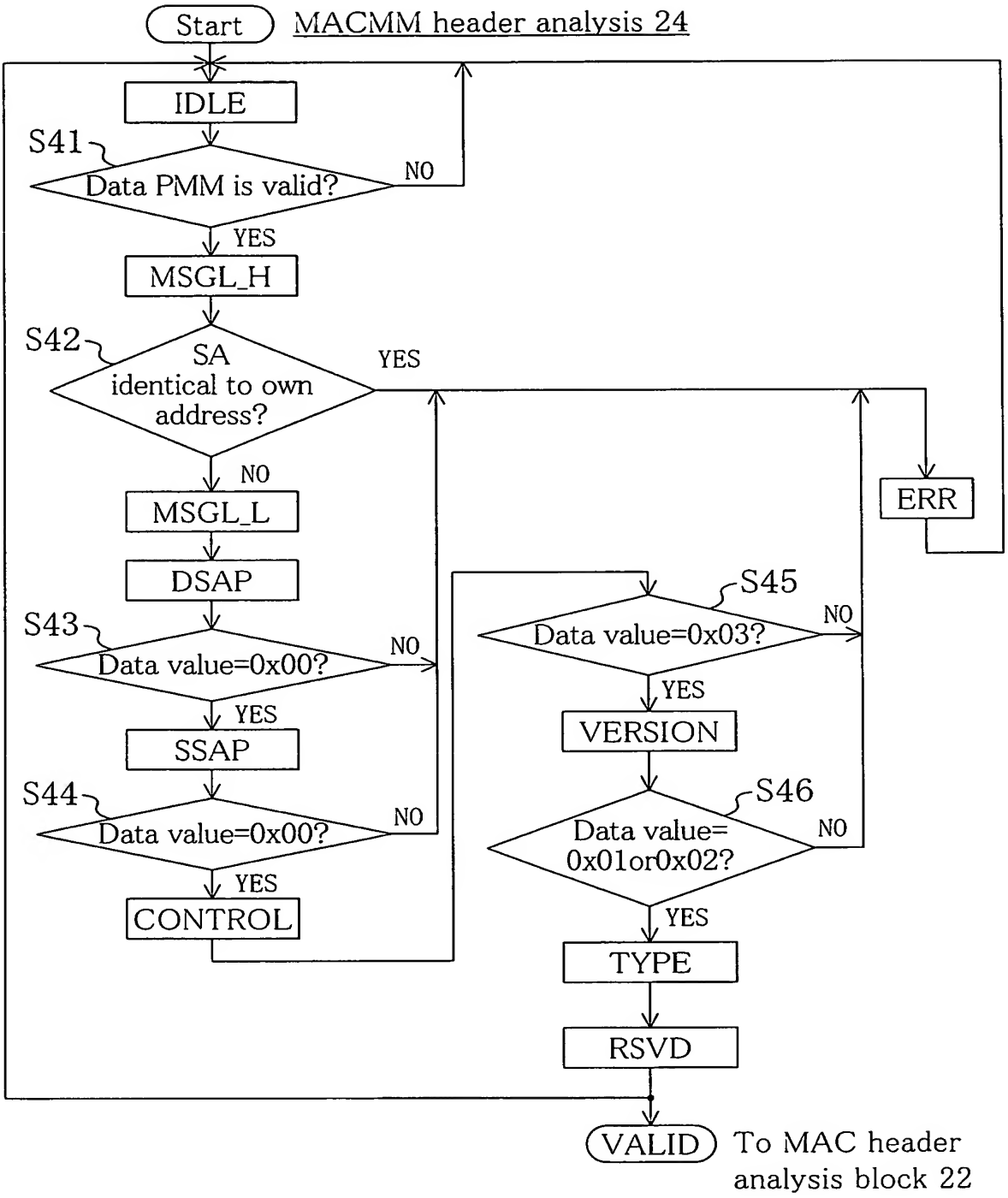

Start
MACMM header analysis 24
IDLE
S41
Data PMM is valid?
NO
YES
MSGL_H
S42
SA identical to own address?
YES
NO
MSGL_L
DSAP
S43
Data value=0x00?
NO
YES
SSAP
S44
Data value=0x00?
NO
YES
CONTROL
ERR
S45
Data value=0x03?
NO
YES
VERSION
S46
Data value= 0x01or0x02?
NO
YES
TYPE
RSVD
VALID
To MAC header analysis block 22

FIG. 13

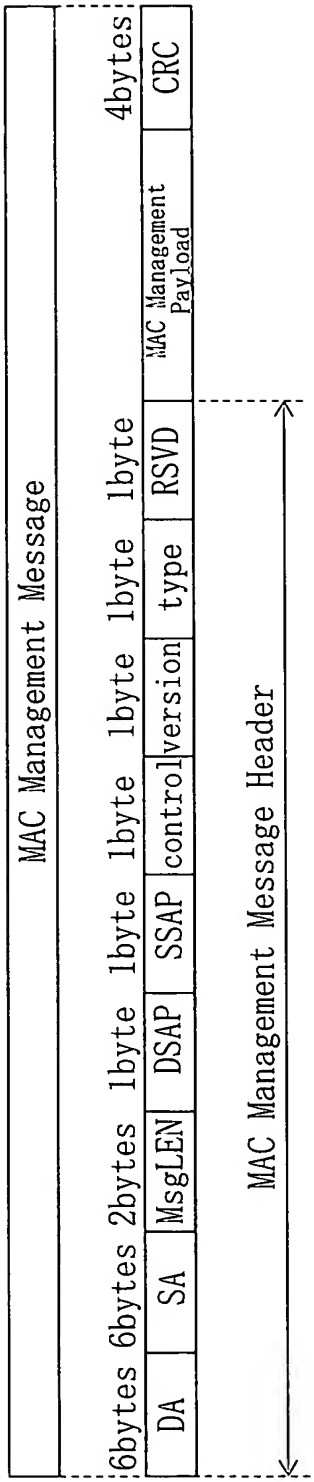
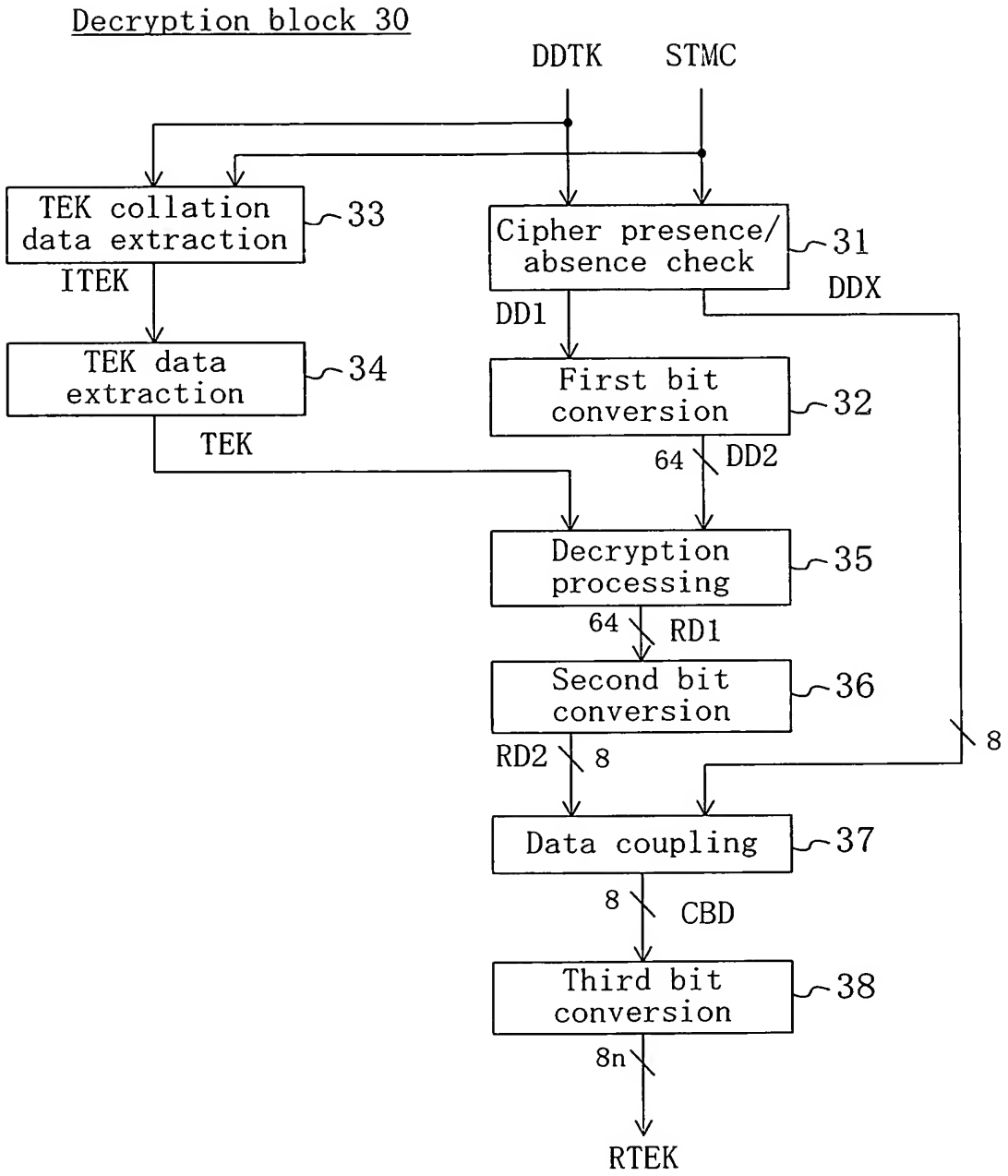

MAC Management Message
6bytes
DA
6bytes
SA
2bytes
MsgLEN
1byte
DSAP
1byte
SSAP
1byte
control
1byte
version
1byte
type
1byte
RSVD
MAC Management Payload
4bytes
CRC
MAC Management Message Header

FIG. 14


Decryption block 30
DDTK
STMC
TEK collation data extraction
33
ITEK
TEK data extraction
34
TEK
Cipher presence/ absence check
31
DDX
DD1
First bit conversion
32
64
DD2
Decryption processing
35
64
RD1
Second bit conversion
36
RD2
8
8
Data coupling
37
8
CBD
Third bit conversion
38
8n
RTEK